IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1-13. (canceled).

14. (currently amended): A security management method for supporting security management of a plurality of managed systems executed in an information system comprised of computers connected through a network, comprising:

designing security specifications to be applied to the information system by using an information security policy designated by a user,

wherein the information security policy is applied to each of the plurality of managed systems designated by the user,

wherein the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures, and

wherein each security measure indicates an action to be taken to secure the managed systems;

auditing a security status of the information system with respect to the information security policy designated by the user,

wherein the security status indicates whether a security measure has been executed;

auditing system information of each of the plurality of managed systems,

wherein the system information comprises a version of a software program installed in each respective managed system, and a type of apparatus in which each respective managed systems operates;

changing the security status of each of the managed systems based on a result of auditing the security status and the system information; and

auditing the security status of the information system and the system information every time a security setting is changed.

15. (previously presented): The security management method according to claim 14, further comprising:

diagnosing the security of the information system by using an audit program selected from a second database, which includes a correspondence between audit programs, the information security policies, the managed systems, and management programs,

wherein each audit program audits the security status of each of said managed systems, and

wherein the management programs manage security measures of the information security policies and are designated by the user when performing the step of designing the security specifications; and

changing, by a management program selected from the second database, the security status of a managed system corresponding to the management program, so as to adjust the security status in accordance with an information security policy corresponding to the management program.

16. (previously presented): The security management method according to claim 14, further comprising:

in accordance with a security setting content received from the user, changing, by a management program selected from a second database, the security status of a managed system corresponding to the management program, so as to adjust the security status in accordance with the information security policy corresponding to the management program,

wherein the second database includes a correspondence between audit programs, the information security policies, the managed systems, and management programs.

17. (currently amended): The security management method according to claim 14, further comprising:

checking the result of auditing against security hole information published by a security information organization ~~such as Computer~~

~~Emergency Response Team (CERT)~~ to determine if a security hole exists; and

changing the security status of the managed system in which ~~a~~ the security hole is found.

18. (currently amended): A security management system for supporting security management of managed systems executed in an information system comprised of computers connected through a network, comprising:

a first database, which includes information regarding the managed systems to which information security policies are applied;

a second database, which includes information regarding specifications of information security policies;

a third database, which includes a correspondence between the managed systems and information security policies;

a management and audit object area control section which selects, from said first database, managed systems to which information security ~~polices~~ policies are applied based on a designation by a user;

an information security policy selection control section which extracts, from said second database, information security policy specifications based on a designation by a user;

an information security policy/security management and audit program correspondence control section that extracts, from said third database, an information security policy corresponding to the managed systems, and

designs security specifications for each of the managed systems by using the information security policy specifications designated by the user;

a plurality of audit sections that audit a security status of the information system with respect to the information security policy designated by the user,

wherein the security status indicates whether a specific action to secure the managed systems has been executed,

wherein the plurality of audit sections further audit system information of the managed systems, and

wherein the system information comprises a version of a software program installed in each respective managed system, and a type of apparatus in which each respective managed systems operates; and

a plurality of management sections that obtain the security status of the information system and the system information, based on audit results from the plurality of audit sections, and manage security status relating to the information security policy of the managed systems in order to bring the security status of the managed systems in conformity with the information security policy specified by the security specification designed at the information security policy/security management and audit program correspondence control section,

wherein the information security policy/security management and audit program correspondence control section audits the security status of the information system and the system information every time a security setting is changed.